American National Standard for Financial Services

ANSI X9.69–2017

Framework for Key Management Extensions

Developed by
Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: September 19, 2017

American National Standards Institute

Contents

Page

Figures

Foreword

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretation should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of approval.

Published by

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
275 West Street, Suite 107
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

Introduction

This Standard is concerned with symmetric key systems in which the encrypting key and decrypting key are identical. The security and reliability of any process based on a symmetric cryptographic algorithm is directly dependent on the protection afforded to the secret quantity, called the key. Thus, no matter how strong the algorithm, the system is only as secure as its key management method.

This Standard defines two specific key management methods for controlling and handling keys, called (1) Constructive Key Management and (2) Key Usage Control. Each method can be used independently; or the methods can be used in combination. However, the combined use of the methods is highly recommended by the ASC X9 Subcommittee responsible for this Standard. Each method is described in a separate section of the Standard.

The section on CONSTRUCTIVE KEY MANAGEMENT, systematizes key creation, implementing “dual control” or “split knowledge” by using key components to construct the final working key. This working key may be used in several ways including as a session key, for a store-and-forward (i.e. e-mail) application, and for file encryption applications, such as archiving, or protecting filed information until needed again by the user. Other applications are also possible. Until now, this practice of split knowledge key creation has been used mainly to transport key parts into systems where “master keys” were used to protect keys in storage, and to recover the working keys for a current application. With the methodology of this Standard, a working key will be created as needed for a specific encryption process, and re-created when needed to decrypt the object. Depending on the application, the key may be saved or destroyed after each use. The working key is never transmitted; the application program only knows it while it is in use.

The section on KEY USAGE CONTROL, allows the creator of a key to specify the allowed uses of the key. For example, key usage control information can be used to distinguish key types (data, PIN, or key-encrypting). The type “data key” can be further sub-divided to distinguish data privacy keys—keys used to encrypt and decrypt data—from Message Authentication Code (MAC) keys---keys used to protect the integrity of data. The method attaches or binds a “key usage vector” to each generated key, for the life of the key, and is used by the system to ensure that keys are used properly. In short, the key usage vector prevents abuses and attacks against the key. The key usage vector can be used to protect keys stored within a single system, or to protect keys transmitted from one system to another.

This Standard is algorithm independent, and as new cryptographic algorithms with perhaps longer key lengths than currently in use are developed and adopted by the Financial Community this Standard will still apply.

This standard includes a Constructive Key Management working key for a symmetric encryption capability. Studies are surfacing that asymmetrical key can be subject to Quantum Computing attack.[1]

NOTE The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights.

By publication of this standard, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the standards developer.

---

[1] NISTIR 8105 Report on Post-Quantum Cryptography Feb 2016

Suggestions for the improvement or revision of this Standard are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, 275 West Street, Suite 107 Annapolis, MD 21401 USA.

This Standard was processed and approved for submittal to ANSI by the Accredited Standards Committee on Financial Services, X9. Committee approval of the Standard does not necessarily imply that all the committee members voted for its approval.

The X9 committee had the following members:

Roy DeCicco, X9 Chairman
Angela Hendershott, X9 Vice-Chairman
Steve Stevens, Executive Director
Janet Busch, Program Manager

Organization Represented ..... *Representative*

ACI Worldwide ..... Doug Grote
ACI Worldwide ..... Dan Kinney
American Bankers Association ..... Diane Poole
American Express Company ..... David Moore
Bank of America ..... Daniel Welch
Bank of New York Mellon ..... Kevin Barnes
Blackhawk Network ..... Anthony Redondo
Bloomberg LP ..... Corby Dear
Capital One ..... Marie LaQuerre
Citigroup, Inc. ..... Karla McKenna
CLS Bank ..... Ram Komarraju
Conexxus, Inc. ..... Michael Davis
Conexxus, Inc. ..... Gray Taylor
CUSIP Service Bureau ..... Gerard Faulkner
Delap LLP ..... Andrea Beatty
Delap LLP ..... Darlene Kargel
Deluxe Corporation ..... Angela Hendershott
Diebold Nixdorf ..... Bruce Chapa
Discover Financial Services ..... Michelle Zhang
eCurrency ..... David Wen
Federal Reserve Bank ..... Mary Hughes
Federal Reserve Bank ..... Janet LaFrence
FIS ..... Stephen Gibson-Saxty
Fiserv ..... Dan Otten
FIX Protocol Ltd - FPL ..... Jim Northey
Futurex ..... Ryan Smith
Gilbarco ..... Bruce Welch
Harland Clarke ..... John McCleary
Hewlett Packard ..... Susan Langford
IBM Corporation ..... Todd Arnold
Independent Community Bankers of America ..... Cary Whaley
Ingenico ..... Rob Martin
ISITC ..... Jason Brasile
J.P. Morgan Chase ..... Roy DeCicco
KPMG LLP ..... Mark Lundin
MagTek, Inc. ..... Roger Applewhite
MagTek, Inc. ..... Mimi Hart
MasterCard Europe Sprl ..... Mark Kamers
NACHA The Electronic Payments Association ..... Priscilla Holland

National Security Agency ..... Paul Timmel
Nautilus Hyosung ..... Joe Militello
NCR Corporation ..... David Norris
Office of Financial Research, U.S. Treasury Department ..... Justin Stekervetz
PCI Security Standards Council ..... Troy Leach
RouteOne ..... Chris Irving
RouteOne ..... Jenna Wolfe
Symcor Inc. ..... Debbi Fitzpatrick
TECSEC Incorporated ..... Ed Scheidt
The Clearing House ..... Sharon Jablon
U.S. Bank ..... John King
U.S. Commodity Futures Trading Commission (CFTC) ..... Robert Stowsky
USDA Food and Nutrition Service ..... Kathy Ottobre
Vantiv LLC ..... Gary Zempich
VeriFone, Inc. ..... Dave Faoro
VISA ..... Kim Wagner
Wayne Fueling Systems ..... Steven Bowles
Wells Fargo Bank ..... Mark Schaffer

The X9F subcommittee on Information Security had the following members:

Dave Faoro, X9F Chair
Sandra Lambert, X9F Vice Chair

Organization Represented	*Representative*
ACI Worldwide	Doug Grote
ACI Worldwide	Dan Kinney
ACI Worldwide	Julie Samson
American Bankers Association	Tom Judd
American Express Company	Farid Hatefi
American Express Company	John Timar
American Express Company	Kevin Welsh
Bank of America	Amanda Adams
Bank of America	Peter Capraro
Bank of America	Andi Coleman
Bank of America	Lawrence LaBella
Bank of America	Will Robinson
Bank of America	Michael Smith
Bank of America	Daniel Welch
BlackBerry Limited	Daniel Brown
BlackBerry Limited	Sandra Lambert
Blackhawk Network	Vijay Bolina
Blackhawk Network	Anthony Redondo
Bloomberg LP	Erik Anderson
Bloomberg LP	Corby Dear
Capital One	Marie LaQuerre
Capital One	Johnny Lee
Cipherithm	Scott Spiker
comForte 21 GmbH	Thomas Gloerfeld
comForte 21 GmbH	Henning Horst
Communications Security Establishment	Jonathan Hammell
Communications Security Establishment	David Smith
Conexxus, Inc.	Alan Thiemann
CUSIP Service Bureau	Scott Preiss
Delap LLP	Andrea Beatty
Delap LLP	David Buchanan
Delap LLP	Darlene Kargel
Deluxe Corporation	Angela Hendershott
Deluxe Corporation	Margiore Romay
Deluxe Corporation	Andy Vo
Diebold Nixdorf	Christoph Bruecher
Diebold Nixdorf	Andrea Carozzi
Diebold Nixdorf	Bruce Chapa
Diebold Nixdorf	Michael Nolte
Diebold Nixdorf	Michael Ott
Diebold Nixdorf	Dave Phister
Discover Financial Services	Cheryl Mish
Discover Financial Services	Diana Pauliks
Discover Financial Services	Jordan Schaefer
eCurrency	David Wen
Federal Reserve Bank	Patrick Adler
Federal Reserve Bank	Guy Berg
Federal Reserve Bank	Marianne Crowe
Federal Reserve Bank	Amanda Dorphy

Federal Reserve Bank ..... Mary Hughes
Federal Reserve Bank ..... Heather Hultquist
Federal Reserve Bank ..... Janet LaFrence
Federal Reserve Bank ..... Susan Pandy
Federal Reserve Bank ..... Patti Ritter
Federal Reserve Bank ..... Daniel Rozycki
First Data Corporation ..... Annmarie Corrigan
First Data Corporation ..... Lisa Curry
First National Bank of Omaha ..... Kristi White
FIS ..... Chelsea Lopez
FIS ..... John Soares
FIS ..... Sunny Wear
Fiserv ..... Bud Beattie
Fiserv ..... Dan Otten
Futurex ..... Ryan Smith
GEOBRIDGE Corporation ..... Donna Gem
GEOBRIDGE Corporation ..... Jason Way
Gilbarco ..... Scott Turner
Gilbarco ..... Bruce Welch
Harland Clarke ..... Joseph Filer
Heartland Payment Systems ..... Scott Meeker
Hewlett Packard ..... Susan Langford
Hewlett Packard ..... Luther Martin
Hewlett Packard ..... Terence Spies
IBM Corporation ..... Todd Arnold
Independent Community Bankers of America ..... Cary Whaley
Ingenico ..... Rob Martin
ITS, Inc. (SHAZAM Networks) ..... Manish Nathwani
J.P. Morgan Chase ..... Bruce Geller
J.P. Morgan Chase ..... Kathleen Krupa
J.P. Morgan Chase ..... Jackie Pagán
J.P. Morgan Chase ..... Darryl Scott
K3DES LLC ..... Azie Amini
KPMG LLP ..... Mark Lundin
MagTek, Inc. ..... Jeff Duncan
MagTek, Inc. ..... Mimi Hart
MasterCard Europe Sprl ..... Mark Kamers
MasterCard Europe Sprl ..... Joshua Knopp
MasterCard Europe Sprl ..... Larry Newell
MasterCard Europe Sprl ..... Adam Sommer
MasterCard Europe Sprl ..... Michael Ward
National Institute of Standards and Technology (NIST) ..... Elaine Barker
National Institute of Standards and Technology (NIST) ..... Lily Chen
National Security Agency ..... Mike Boyle
National Security Agency ..... Paul Timmel
Nautilus Hyosung ..... Joe Militello
Nautilus Hyosung ..... Jay Shin
NCR Corporation ..... Tanika Eng
NCR Corporation ..... Charlie Harrow
NCR Corporation ..... David Norris
Onboard Security ..... Mark Etzel
Onboard Security ..... William Whyte
Onboard Security ..... Lee Wilson
Onboard Security ..... Zhenfei Zhang
PCI Security Standards Council ..... Leon Fell
PCI Security Standards Council ..... Troy Leach

PCI Security Standards Council ..... Ralph Poore
RSA, The Security Division of EMC ..... Steve Schmalz
SafeNet, Inc. ..... Amit Sinha
TECSEC Incorporated ..... Ed Scheidt
TECSEC Incorporated ..... Dr. Wai Tsang
TECSEC Incorporated ..... Jay Wack
Thales UK Limited ..... Larry Hines
Thales UK Limited ..... James Torjussen
The Clearing House ..... Henry Farrar
The Clearing House ..... Sharon Jablon
Trustwave ..... John Amaral
Trustwave ..... Tim Hollebeek
U.S. Bank ..... Stephen Case
U.S. Bank ..... Peter Skirvin
Vantiv LLC ..... Jeffrey Singleton
Vantiv LLC ..... Bill Weingart
Vantiv LLC ..... Gary Zempich
Vantiv LLC ..... James Zerfas
VeriFone, Inc. ..... John Barrowman
VeriFone, Inc. ..... David Ezell
VeriFone, Inc. ..... Dave Faoro
VeriFone, Inc. ..... Doug Manchester
VeriFone, Inc. ..... Brad McGuinness
VeriFone, Inc. ..... Joachim Vance
VISA ..... Shahzad Khan
VISA ..... Kim Wagner
Wayne Fueling Systems ..... Steven Bowles
Wells Fargo Bank ..... William Felts, IV
Wells Fargo Bank ..... Phillip Griffin
Wells Fargo Bank ..... Jan Kohl
Wells Fargo Bank ..... Garrett Macey
Wells Fargo Bank ..... Kelly O'Donnell
Wells Fargo Bank ..... Mark Schaffer
Wells Fargo Bank ..... Jeff Stapleton
XYPRO Technology ..... Steve Tcherchian

Under ASC X9, Inc. procedures, a working group may be established to address specific segments of work under the ASC X9 Committee or one of its subcommittees. A working group exists only to develop standard(s) or guideline(s) in a specific area and is then disbanded. The individual experts are listed with their affiliated organizations. However, this does not imply that the organization has approved the content of the standard or guideline. (Note: Per X9 policy, company names of non-member participants are listed only if, at the time of publication, the X9 Secretariat received an original signed release permitting such company names to appear in print.)

The X9F4 Cryptographic Protocol and Application Security working group which developed this standard had the following members:

Jeff Stapleton, X9F4 Chair
Sandra Lambert, X9F4 Vice Chair

Organization Represented — *Representative*

Bank of America ..... Amanda Adams
Bank of America ..... Peter Capraro

Bank of America ..... Andi Coleman
Bank of America ..... David Freeman
Bank of America ..... Lawrence LaBella
Bank of America ..... Daniel Welch
BlackBerry Limited ..... Daniel Brown
BlackBerry Limited ..... Sandra Lambert
Bloomberg LP ..... Erik Anderson
Capital One ..... Johnny Lee
Cipherithm ..... Scott Spiker
comForte 21 GmbH ..... Henning Horst
Conexxus, Inc. ..... Alan Thiemann
Conexxus, Inc. ..... Linda Toth
Delap LLP ..... Andrea Beatty
Delap LLP ..... Darlene Kargel
Diebold Nixdorf ..... Christoph Bruecher
Diebold Nixdorf ..... Rick Brunt
Diebold Nixdorf ..... Andrea Carozzi
Diebold Nixdorf ..... Bruce Chapa
Diebold Nixdorf ..... Scott Harroff
Diebold Nixdorf ..... Anne Konecny
Diebold Nixdorf ..... Michael Nolte
Diebold Nixdorf ..... Michael Ott
Diebold Nixdorf ..... Dave Phister
Diebold Nixdorf ..... Matthias Runowski
Discover Financial Services ..... Cheryl Mish
Discover Financial Services ..... Diana Pauliks
Discover Financial Services ..... Lakshmi Ramanathan
Discover Financial Services ..... Jordan Schaefer
Discover Financial Services ..... Michelle Zhang
Federal Reserve Bank ..... Patrick Adler
Federal Reserve Bank ..... Guy Berg
Federal Reserve Bank ..... Marianne Crowe
Federal Reserve Bank ..... Pieralberto Deganello
Federal Reserve Bank ..... Amanda Dorphy
Federal Reserve Bank ..... Mary Hughes
Federal Reserve Bank ..... Heather Hultquist
Federal Reserve Bank ..... Janet LaFrence
Federal Reserve Bank ..... Paul Nunnally
Federal Reserve Bank ..... Susan Pandy
Federal Reserve Bank ..... Patti Ritter
Federal Reserve Bank ..... Daniel Rozycki
Federal Reserve Bank ..... Charles Tsai
First Data Corporation ..... Lisa Curry
First Data Corporation ..... Brian Kean
First Data Corporation ..... Brian Murray
First Data Corporation ..... Randall Rieth
FIS ..... Chelsea Lopez
FIS ..... Ian Lumsden
FIS ..... Sunny Wear
Fiserv ..... Dan Otten
FIX Protocol Ltd - FPL ..... Jim Northey
GEOBRIDGE Corporation ..... Donna Gem
GEOBRIDGE Corporation ..... Dean Macinskas
GEOBRIDGE Corporation ..... Jason Way
Gilbarco ..... Bruce Welch
Harland Clarke ..... John McCleary

Hewlett Packard ..... Terence Spies
IBM Corporation ..... Todd Arnold
Independent Community Bankers of America ..... Cary Whaley
ITS, Inc. (SHAZAM Networks) ..... Manish Nathwani
J.P. Morgan Chase ..... Robin Doyle
J.P. Morgan Chase ..... Darryl Scott
K3DES LLC ..... Davi Ottenheimer
KPMG LLP ..... Mark Lundin
MagTek, Inc. ..... Mimi Hart
MasterCard Europe Sprl ..... Mark Kamers
Merchant Advisory Group ..... Brad Andrews
National Institute of Standards and Technology (NIST) ..... Elaine Barker
National Institute of Standards and Technology (NIST) ..... Lily Chen
National Institute of Standards and Technology (NIST) ..... Elaine Newton
National Institute of Standards and Technology (NIST) ..... Burak Sahin
National Security Agency ..... Greg Gilbert
National Security Agency ..... Tim Havighurst
National Security Agency ..... Paul Timmel
NCR Corporation ..... Charlie Harrow
NCR Corporation ..... Brian Wotherspoon
Onboard Security ..... Mark Etzel
Onboard Security ..... Jeff Hoffstein
Onboard Security ..... William Whyte
PCI Security Standards Council ..... Leon Fell
PCI Security Standards Council ..... Troy Leach
PCI Security Standards Council ..... Ralph Poore
PCI Security Standards Council ..... Elizabeth Terry
RSA, The Security Division of EMC ..... Steve Schmalz
SafeNet, Inc. ..... Amit Sinha
TECSEC Incorporated ..... Ed Scheidt
TECSEC Incorporated ..... Dr. Wai Tsang
TECSEC Incorporated ..... Jay Wack
Thales UK Limited ..... Colette Broadway
Thales UK Limited ..... Larry Hines
Thales UK Limited ..... James Torjussen
The Clearing House ..... Ken Friedman
The Clearing House ..... Sharon Jablon
Trustwave ..... Tim Hollebeek
U.S. Bank ..... Stephen Case
U.S. Bank ..... Peter Skirvin
Vantiv LLC ..... Gary Zempich
VeriFone, Inc. ..... David Ezell
VeriFone, Inc. ..... Dave Faoro
VeriFone, Inc. ..... LeAnn Hostetler
VeriFone, Inc. ..... Doug Manchester
VeriFone, Inc. ..... Joachim Vance
VISA ..... Geoff Brookman
VISA ..... Hap Huynh
VISA ..... Shahzad Khan
VISA ..... Chackan Lai
VISA ..... Johan ("Hans") Van Tilburg
VISA ..... Kim Wagner
Wells Fargo Bank ..... Sotos Barkas
Wells Fargo Bank ..... Tony Bautts
Wells Fargo Bank ..... William Felts, IV
Wells Fargo Bank ..... Phillip Griffin

Wells Fargo Bank..... Sam Grosby
Wells Fargo Bank..... Jeff Jacoby
Wells Fargo Bank.....Joseph Kaluzny
Wells Fargo Bank.....Brian Keltner
Wells Fargo Bank..... Jan Kohl
Wells Fargo Bank.....Eric Lengvenis
Wells Fargo Bank.....Doug Pelton
Wells Fargo Bank..... Mike Rudolph
Wells Fargo Bank..... Jeff Stapleton
Wells Fargo Bank.....Tony Stieber
Wells Fargo Bank..... Nathan Suri

This document cancels and replaces the original X9.69-1999 Framework for Key Management Extensions and its successor X9.69-2006 in whole. X9.69-2006 and now this standard were revised to address the industry transition from single DES to TDEA and AES, with the following changes:

A. Reference to the following documents were added:
   - SP800-67 Recommendations for the Triple Data Encryption Algorithm (TDEA) Block Cipher [2.1]
   - FIPS 197 Advanced Encryption Standard (AES) [2.5]
   - IEEE Cryptography Transitions
   - X9.102 Symmetric Key Cryptography For the Financial Services Industry – Wrapping of Keys and Associated Data [2.3]
   - TR-31 Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms [2.4]
   - NISTIR 8105 Report on Post Quantum Cryptography
   - NIST SP800-162 Guidelines for Attribute Based Access Control

B. References to the following withdrawn X9 standards were deleted:
   - X9.9 Financial Institution Message Authentication Codes (MAC) Wholesale; refer to Technical Guideline: Technical Guideline: Managing Risk and Migration Planning: Withdrawal of ANSI X9.9 (X9 TG-24-1999)
   - X9.17 Financial Institution Key Management (Wholesale); refer to Technical Guideline: Managing Risk and Migration Planning: Withdrawal of ANSI X9.17 (X9 TG-26 – 1999)
   - X3.92 Data Encryption Algorithm
   - X3.106 Data Encryption Algorithm – Modes of Operation

C. The follow terms were changed:
   - Policy Manager was changed to CKM Administration
   - Labels was changed to Credentials
   - Credential Manager was changed to Token Distribution

D. The document was converted to the current X9/ISO standards template.

Framework for Key Management Extensions

1 Scope

This Standard defines methods for the generation and control of keys used in symmetric cryptographic algorithms. The Standard defines a *constructive method* for the creation of symmetric keys, by combining two or more secret key components. The Standard also defines a method for attaching a *key usage vector* to each generated key that prevents abuses and attacks against the key. The two defined methods can be used separately or in combination.

The Standard does not cover aspects of key management, such as:

- Key establishment mechanisms;

  See for example ANSI X9.24 Financial Institution Retail Key Management, or ISO/IEC 11770-2, Key Management, Part 2: Mechanisms using symmetric techniques.

- Mechanisms to store, archive, delete, destroy, etc. keys;

- Mechanisms for key recovery in the event of the failure or loss of keys.

The Standard also does not define the implementation of key management mechanisms; there may be different products that comply with this Standard and yet are not interoperable.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

2.1 ANS X9.19 Financial Institution Retail Message Authentication

2.2 SP800-67 Recommendations for the Triple Data Encryption Algorithm (TDEA) Block Cipher

2.3 SP800-162 Recommendations for Attribute Based Access Control

2.4 ANS X9.102 Symmetric Key Cryptography For the Financial Services Industry – Wrapping of Keys and Associated Data

2.5 ANS TR-31 Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

2.6 FIPS 197 Advanced Encryption Standard (AES)

2.7 ANSI X9.73 Cryptographic Message Syntax for XML and ASN.1

2.8 ANSI X9.112 Security for Wireless Communiations

2.9 ANSI X9.125 Cloud Security